Claims

1. An intrusion secure computer system comprising:
   a CPU;
   a data storage means;
   a memory means;
   an operating system;
   a virtual machine operating system; and
   at least one I/O connection in operative communication with a data source.

2. The computer system of claim 1, wherein the data source is a global computer network.

3. The computer system of claim 1, wherein the data source is other than a global computer network.

4. The computer system of claim 3, wherein the data source other than a global computer network is at least one data source selected from the group consisting of: a computer workstation, a personal-type computer, a computer dock, a local area network, an intranet, and a wide area network.

5. The intrusion secure computer system of claim 1, wherein the virtual machine operating system comprises software for defining a virtual machine environment in memory and a virtual drive in storage, and operational control software limiting operative communication with the data source to the virtual machine environment and the virtual machine drive.

6. A method for securing a computer system from intrusion from an external data source comprising the steps of:
   providing an intrusion secure computer system of claim 1;
   initiating an external data source interface session, and causing activation of a virtual machine operating system of claim 1 and defining a virtual

machine environment in memory and a virtual drive in storage; and establishing connectivity with the external data source under control of the virtual machine operating system to isolate operative communication with the external data source to the virtual machine environment and the virtual drive to secure the computer system from intrusion from the external data source.

7. A software application installable on a personal computer, the software protecting the computer's primary data files from being accessed by malicious code from an external data source, the software comprising:

computer code for a isolated operating environment; and

computer code for a secondary operating system functional within the isolated operating environment.

8. The software application of claim 7, wherein the isolated operating environment computer code includes POS permission code for modifying the POS permissions.

9. The software application of claim 8, wherein the secondary operating system computer code includes POS permission code for modifying POS external data source related access permissions.

10. The software application of claim 9, wherein the secondary operating system computer code includes POS permission code for modifying POS external data source related access permissions, wherein the external data source is at least one source selected from the group consisting of a network node, an external data device, and an I/O device.

11. The software application of claim 8, wherein the secondary operating system computer code includes POS permission code for modifying POS internet related permissions.

12. The software application of claim 8, wherein the secondary operating system computer code includes POS permission code for modifying POS Inet permissions.

13. The software application of claim 7, wherein the isolated operating environment computer code includes installation code for checking and setting the isolated operating environment.

14. The software application of claim 13, wherein the isolated operating environment computer code includes installation code for checking and setting the isolated operating environment, wherein the installation code checks for the current installation condition of the software application.

15. The software application of claim 14, wherein the isolated operating environment computer code includes installation code for checking and setting the isolated operating environment, wherein the installation code copies any files from the software application as are necessary in view of the check for current installation condition of the software application.

16. The software application of claim 14, wherein the isolated operating environment computer code includes installation code for checking and setting the isolated operating environment, wherein the installation code establishes short-cuts as are necessary in view of the check for current installation condition of the software application.

17. The software application of claim 7, wherein the isolated operating environment computer code includes code checking and setting the isolated operating environment start up requirements.

18. The software application of claim 17, wherein the isolated operating environment computer code includes code checking and setting the isolated

operating environment start up requirements regarding "freshness" of the SOE files, allocation of volatile memory to the SOE, allocation of data storage to the SOE, READ ONLY condition of the primary operating system partitions and connections, state of intranet activity, READ ONLY condition of user access to primary operating system partitions.

19. The software application of claim 7, wherein the isolated operating environment computer code includes code checking and setting the isolated operating environment runtime requirements.

20. The software application of claim 19, wherein the isolated operating environment computer code includes code checking and setting the isolated operating environment runtime requirements to provide at least two run modes.

21. The software application of claim 19, wherein the isolated operating environment computer code includes code checking and setting the isolated operating environment runtime requirements to provide at least a run mode with inet access and a run mode without inet access.

22. The software application of claim 7, wherein the isolated operating environment computer code includes code checking and setting the isolated operating environment exit requirements.

23. The software application of claim 22, wherein the isolated operating environment computer code includes code checking and setting the isolated operating environment exit requirements includes disconnecting (the SOE) from the inet, closing the node interface, freeing the SOE volatile memory allocation, flush the temporary data storage allocation, disconnect from any SOE files and partitions, refresh SOE boot file, and restore intranet connection.

24. The software application of claim 7, wherein the isolated operating environment computer code includes code checking and setting the isolated operating environment requirements.

25. The software application of claim 7, wherein the isolated operating environment computer code includes code checking and setting the isolated operating environment requirements, including: allocating and connecting to a region of volatile memory for the SOE, allocating and connecting to a data storage space, providing a connection to a CPU of the computer, connecting to an external data source node, providing a connection to a video card of the computer, providing a connection to a sound card of the computer, providing a connection to a printer of the computer, providing a connection to a mouse and a keyboard of the computer, and forming a network bridge between the secondary operating system of the SOE and the primary operating system of the computer.

26. A security method for protecting a personal computer from malicious code derived from an external data source comprising the steps of:

loading a software application installable on the personal computer, the software application for protecting the computer's primary data files from being accessed by malicious code from an external data source;

installing the software application on the personal computer, the installed application defining a isolated operating environment including a secondary operating system, the secondary operating system functioning in conjunction with and separate from a primary operating on the computer, and the installed application defining primary operating system permission codes to limit access to a node connectable to an external data source to the isolated operating environment under control of the secondary operating system;

initiating an external data source interface session via the node within the isolated operating environment, and allocating a volatile memory space and a temporary data storage space to the secondary operating system for the

duration of the session; and

establishing connectivity with the external data source via the node under control of the secondary operating system to isolate operative communication with the external data source to the isolated operating environment, and protecting the personal computer from malicious code derived from the external data source.